FortiOS™ Handbook

FortiGuard Licensing for FortiGates with Limited or No Connectivity

FortiOS™ Handbook - FortiGuard Licensing for FortiGates with Limited or No Connectivity

October 10, 2014

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of contents

Change Log

Date	Change Description
2014-10-10	Official release.

Introduction

If you purchased FortiGuard services and registered your FortiGate unit, a FortiGate connected to the Internet should automatically connect to the FortiGuard Distribution Network (FDN) to validate the license and download FDN updates. In some high security environments however, Internet service from internal FortiGate appliances is restricted. This document will describe how to configure FortiGate in these situations to allow a local FortiManager appliance to provide both license validation and FDN updates.

This document assumes internal FortiGate appliances have no Internet connectivity, but can access a local FortiManager physical or virtual appliance. It will cover the following:

- Configuring FortiManager as a local FDN
  - With Internet connectivity (including through a Proxy Server)
  - Without Internet connectivity (aka Closed Network Mode)
- Configuring FortiGate to access a local FortiManager as FDN
- Useful troubleshooting commands

Preliminary Steps

1. Register the FortiGate with Fortinet Support under **Asset > Register/Renew**. For a physical FortiGate appliance, enter the serial number. For a FortiGate virtual machine, enter the registration number. Finish the steps to complete registration.
2. For FortiGate VMs, the registration process creates a unique license file that is available under **Asset > View/Manage Products**. Select the correct device, and download the license file.

The following procedures summarize the steps in the FortiManager 5.2.0 Administration Guide section "Connecting the built-in FDS to the FDN".

Configuring FortiManager *with* Internet connectivity as a local FDN server

Follow this procedure to configure a FortiManager with Internet access as a local FDN Server:

1. From the FortiManager GUI, select **System Settings > Network**.
2. Check the following Service Access options on interfaces that will serve FortiGates as the local FDN server:
   - FortiGate Updates
   - Web Filtering/Anti-Spam

3. From the FortiManager GUI, select **FortiGuard > Advanced Settings**.
4. Enable the types of FDN services that you want to provide through FortiManager's built-in FDS by selecting:
   - Enable AntiVirus and IPS Service
   - Enable Web Filter Service
   - Enable Email Filter Service
5. Select **Apply**.

A green Synchronized checkmark appears when the built-in FDS is enabled, and FDN package downloads are successfully completed.

Add these steps to configure FortiManager to access FDN services through a Proxy Server:

6. Expand FortiGuard AntiVirus and IPS Settings.
   a. Check Use Web Proxy.
   b. Enter the IP address and credentials for the Proxy server.
7. Expand FortiGuard Web Filter and Email Filter Settings.
   a. Check Use Web Proxy.
   b. Enter the IP address and credentials for the Proxy server.

Configuring FortiManager *without* Internet connectivity as a local FDN server

FortiManager must have Internet connectivity (direct or via Proxy) to automatically download FDN updates and verify licenses. However, you can manually upload FDN updates and licenses to FortiManager. Known as "Closed Network Mode", this feature allows FortiManager to provide FDN updates and validate licenses to local FortiGate appliances without Internet access.

Follow this procedure to Configure FortiManager in Close Network Mode:

1. Verify that your model of FortiManager supports Closed Network Mode. Review the Features section of the FortiManager Product Data Sheet.
2. To enable Closed Network Mode in FortiManager:

   From the FortiManager GUI, select **FortiGuard > Advanced Settings > Check Disable Communication with FortiGuard Servers**.

   Or from the FortiManager CLI, enable Closed Network Mode by disabling FDS access from the public FDN:

   ```
   config fmupdate publicnetwork
   ```

```
        set status disable
    end
```

Once in Closed Network Mode, FortiManager service packages, updates, and license upgrades must be imported manually.

Follow this procedure to manually upload FortiGate license validation information to FortiManager in Close Network Mode:

1. Create a Customer Service ticket with Fortinet Support under **Assistance > Create Ticket > Customer Service > Submit Ticket**.
2. Enter the Serial Number. Under **Category**, select **CS Contact/License**.
3. In the **Comment** field, ask for an **"entitlement file"** for the FortiGate. Provide the serial number and license number available in **Asset > Manage View Products > <Select product>**.

   Example:
   Serial Number: FGVM010000024628
   License Number: FGVM0035444

As with Asset Registration, for large numbers of FortiGates you can attach a spreadsheet of serial and license numbers for Customer Service. They will provide a single Entitlement File that contains validation information for all included FortiGates. All FortiGates must be registered under the same account – devices registered under different accounts cannot be combined into the same Entitlement File.

4. You will soon receive an Entitlement File from Customer Service.
5. In FortiManager, navigate to **FortiGuard > Advanced Settings > Upload Options for FGT > Service License**and upload d the Entitlement File.

Follow this procedure to manually upload FortiGate AntiVirus/IPS Packages to FortiManager in Close Network Mode:

1. From Fortinet Support, navigate to **Download > FortiGuard Service Updates**. Download the **Virus Definition** and **Attack Definition** files for the appropriate version of FortiGate and FortiOS. These files are named in the form vsigupdate*.pkg and nids*.pkg.
2. In FortiManager, navigate to **FortiGuard > Advanced Settings > Upload Options for FGT > AntiVirus/IPS Packages** and upload the files.

Configuring FortiGate *without* Internet connectivity to access a local FortiManager as FDN

By default, FortiGate connects to the public FDN to validate its license and download security feature updates, including databases and engines for AntiVirus, IPS, etc. FortiGate can be configured to use a local FortiManager for both license validation and FDN updates.

In the case of a FortiGate with no Internet access, the full configuration must be done **before** the license is uploaded. The moment FortiGate receives a license file (via the GUI or CLI), it immediately attempts to access the public FDN to validate the license. Until successful (e.g. there is no timeout), an administrator is unable to login to the GUI and some CLI commands become unavailable (including those needed to define a local FDN server). This makes it very difficult to add the necessary commands to point the FortiGate to a local FortiManager for license validation.

This document will describe the correct way to configure a FortiGate for local FDN access, and a workaround to fix a FortiGate that is unable to access a public license validation server.

Follow this procedure to configure a FortiGate to use a local FortiManager for FDN access:

Completing these steps in a different order may cause the process to fail, and make the FortiGate unable to validate it's license.

From the FortiGate CLI:

1. Configure central management settings:

```
config system central-management
     config server-list
          edit 1
               set server-type update rating
               set server-address <fortimanager_ip>
          next
     end
     set include-default-servers disable
end
```

2. Upload the license using TFTP (or via the GUI):

```
execute restore vmlicense tftp <filename>.lic <tftp_ip>
```

   The FortiGate will reboot.

3. Complete the central management configuration:

```
config system central-management
     set fmg <fortimanager_ip>
end
```

From the FortiManager GUI:

1. Add the FortiGate under **Device Manager > Devices & Groups > Unregistered Devices**. Right-click on the FortiGate and choose **Add**.
2. Select the correct ADOM, enter proper credentials and other settings, and select **OK**.

Follow this procedure to fix a FortiGate that is unable to access a public FDN server:

1. Complete the sections above to ensure the FortiManager is properly configured to service local FortiGates.
2. From the FortiGate CLI, configure the FortiGate to be managed by FortiManager:

```
config system central-management
     set fmg <fortimanager_ip>
end
```

From the FortiManager GUI:

1. Add the FortiGate under **Device Manager > Devices & Groups > Unregistered Devices**. Right-click on the FortiGate and choose **Add**.
2. Select the correct ADOM, enter proper credentials and other settings, and select **OK**.
3. Configure local FDN access by selecting **Device Manager > Provisioning Templates > System Templates > Default**.
4. In the right-hand pane, find the **FortiGuard Widget** (bottom of right column by default).
   a. Check **Enable FortiGuard Security Updates**.
   b. Select the radio button for **Retrieve updates from this FortiManager**.
   c. Deselect **Include Default Servers**.
   d. Click **New**, and enter the IP address of the FortiManager.
   e. Select the radio button for **Updates and Rating**.
   f. Click **OK**, and **Apply**.
5. Assign the Fortigate to this template. On the menu bar of the right pane, select the **Edit** link next to **Assign Devices**.
6. Select the FortiGate in the list of **Devices**, and click **OK**.
7. Apply the template. Navigate to the FortiGate by selecting the correct ADOM and selecting **Devices & Groups > Managed FortiGates**.
8. Right-click on the FortiGate's name, and choose **Install**.
9. Select **Install Device Settings (only)**. Then click **Next**.
10. Complete the wizard and choose **Install**.

Troubleshooting

The following commands can be useful for determining the state of license validation and FDN service connectivity, and gathering information about any connectivity failures. For additional troubleshooting commands, download the FortiOS 5.2 CLI Reference and FortiManager 5.2.0 CLI Reference.

On FortiGate:

- `get system status`
- `get webfilter status`
- `get system auto-update version`
- `get system auto-update status`

On FortiGate-VM:

- `diagnose hardware sysinfo vm full`
- `diagnose debug vm-print-license`
- `diagnose hardware sysinfo vminfo`

On FortiManager:

- `diagnose fmupdate vm-license`